FIG. 1

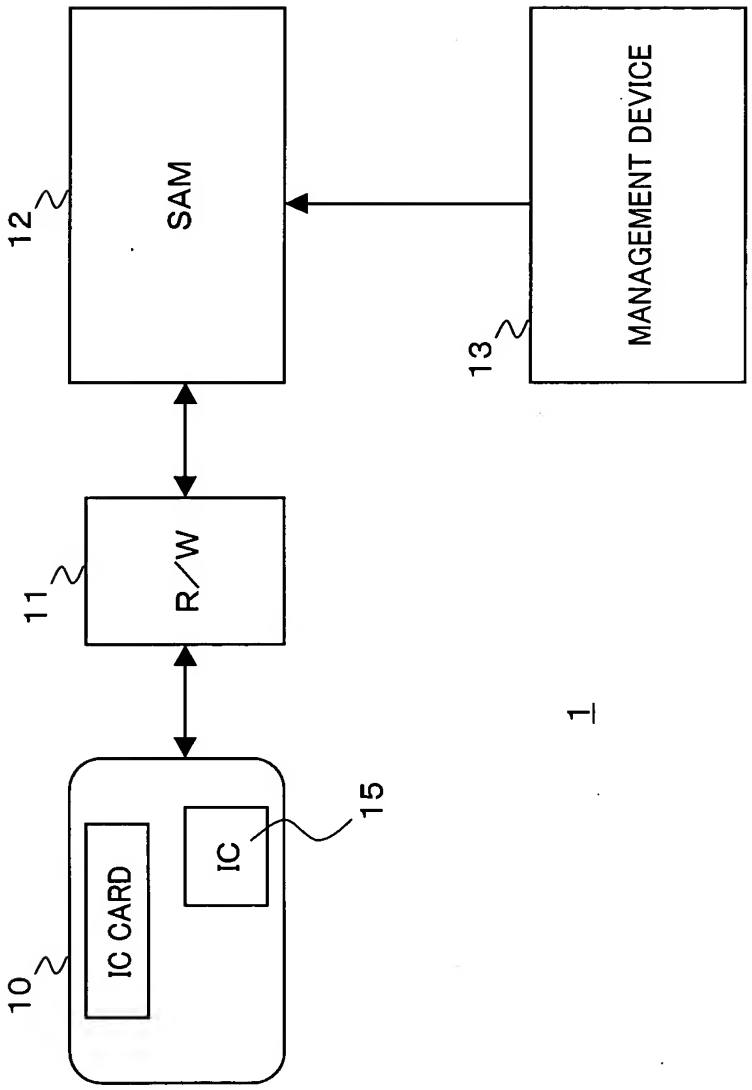


FIG. 2

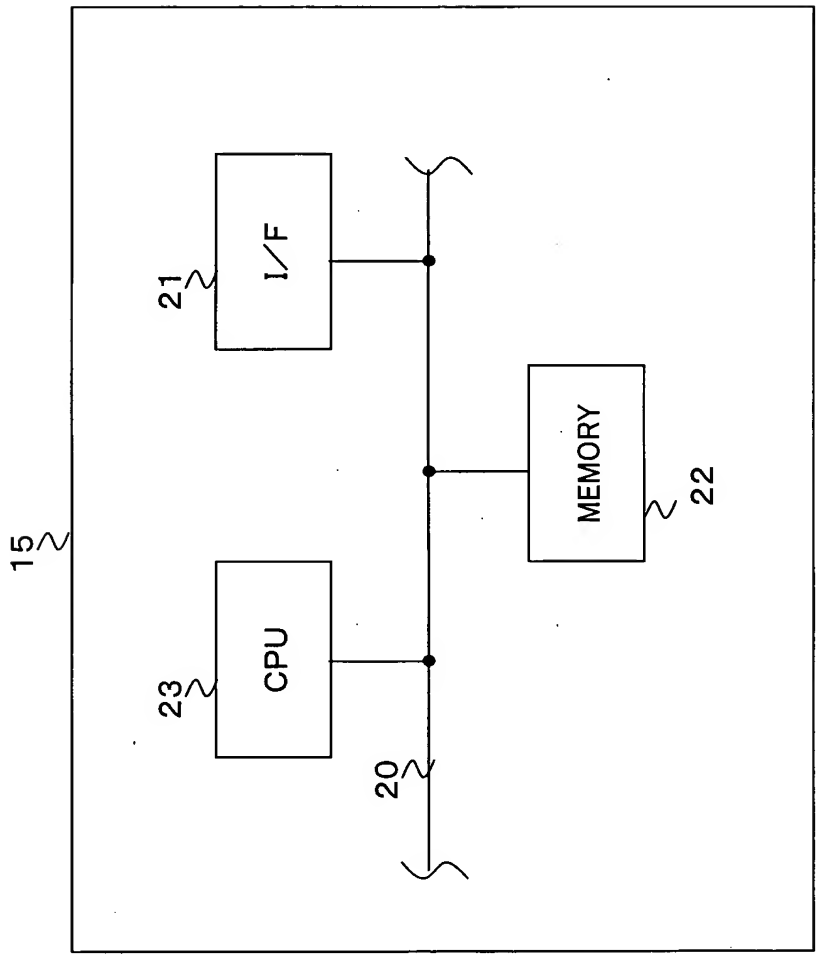


FIG. 3

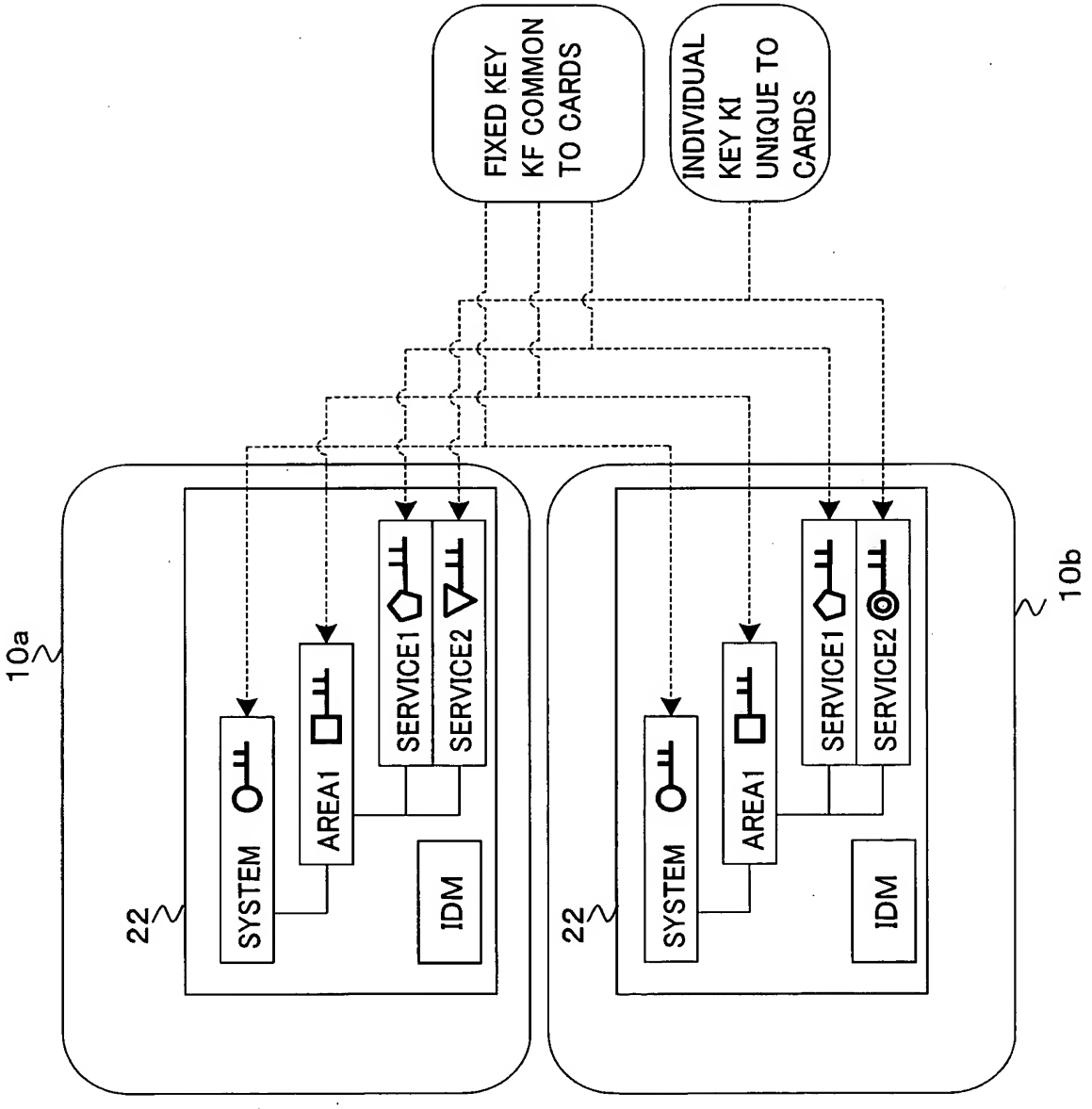

FIXED KEY
KF COMMON
TO CARDS
INDIVIDUAL
KEY KI
UNIQUE TO
CARDS
10a
10b
22
22
SYSTEM
AREA1
SERVICE1
SERVICE2
IDM
SYSTEM
AREA1
SERVICE1
SERVICE2
IDM

FIG. 4

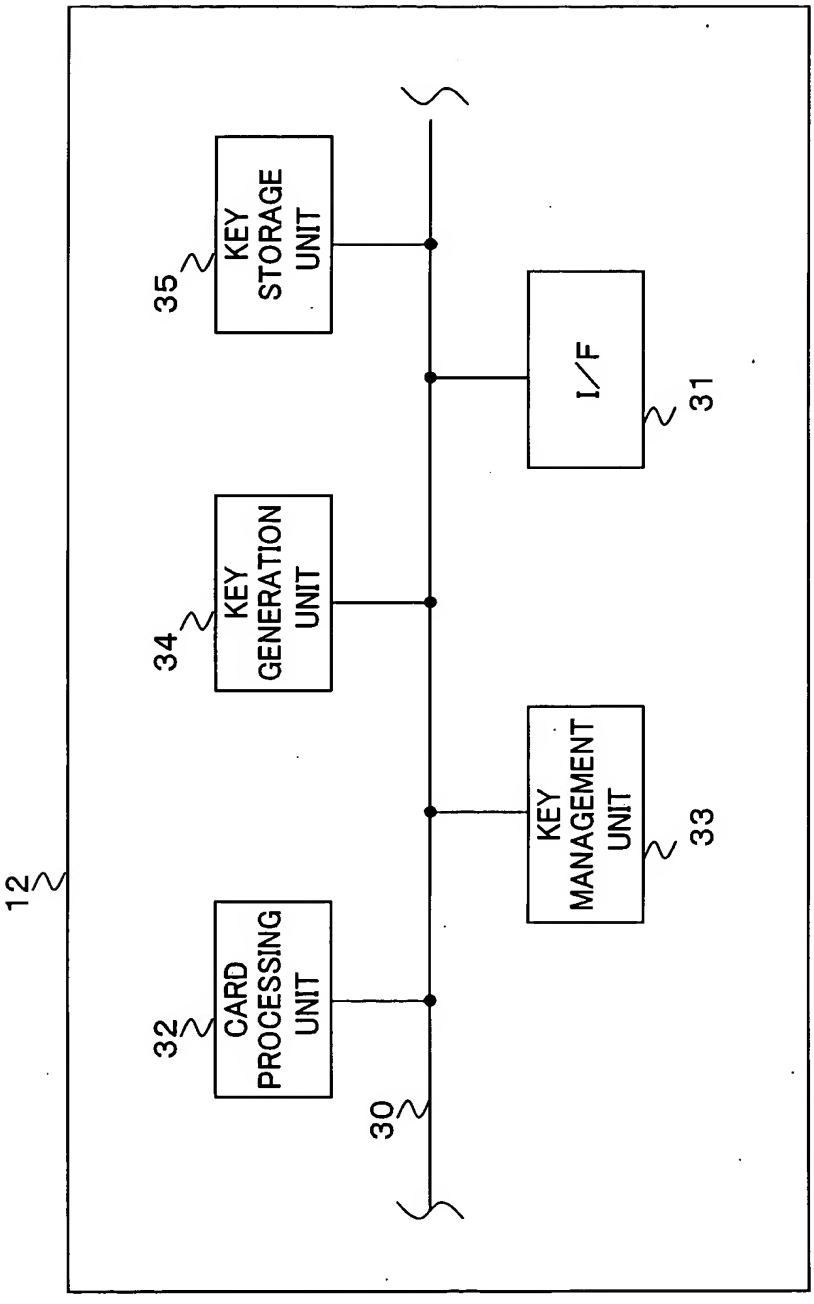

12
KEY STORAGE UNIT
35
I/F
31
KEY GENERATION UNIT
34
KEY MANAGEMENT UNIT
33
CARD PROCESSING UNIT
32
30

FIG. 5

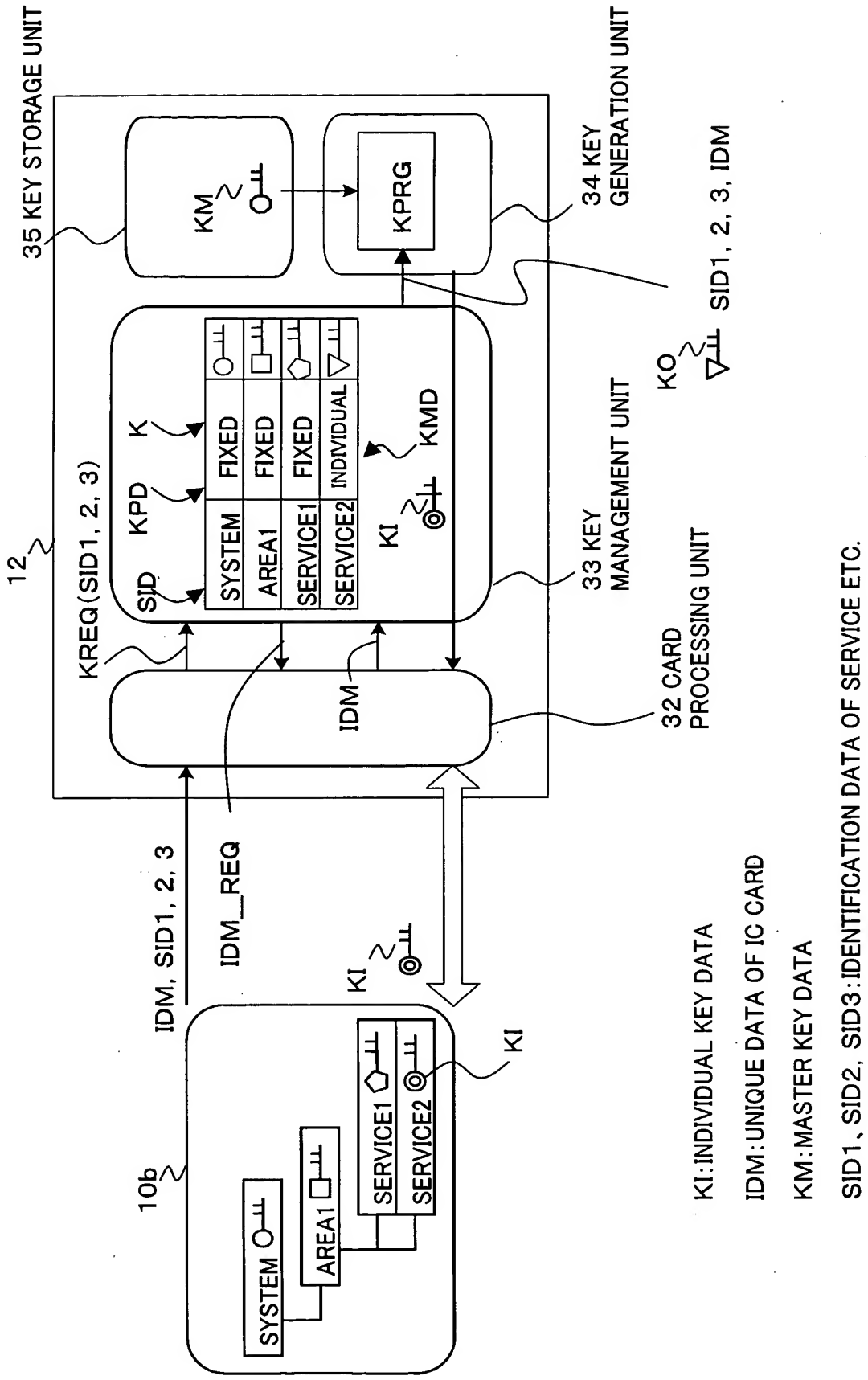

35 KEY STORAGE UNIT
KM
KPRG
34 KEY GENERATION UNIT
12
KREQ(SID1, 2, 3)
SID
KPD
K
SYSTEM
AREA1
SERVICE1
SERVICE2
FIXED
FIXED
FIXED
INDIVIDUAL
KMD
KI
33 KEY MANAGEMENT UNIT
KO
SID1, 2, 3, IDM
IDM
32 CARD PROCESSING UNIT
IDM, SID1, 2, 3
IDM_REQ
KI
KI
10b
SYSTEM
AREA1
SERVICE1
SERVICE2
KI: INDIVIDUAL KEY DATA
IDM: UNIQUE DATA OF IC CARD
KM: MASTER KEY DATA
SID1、SID2、SID3: IDENTIFICATION DATA OF SERVICE ETC.

FIG. 6

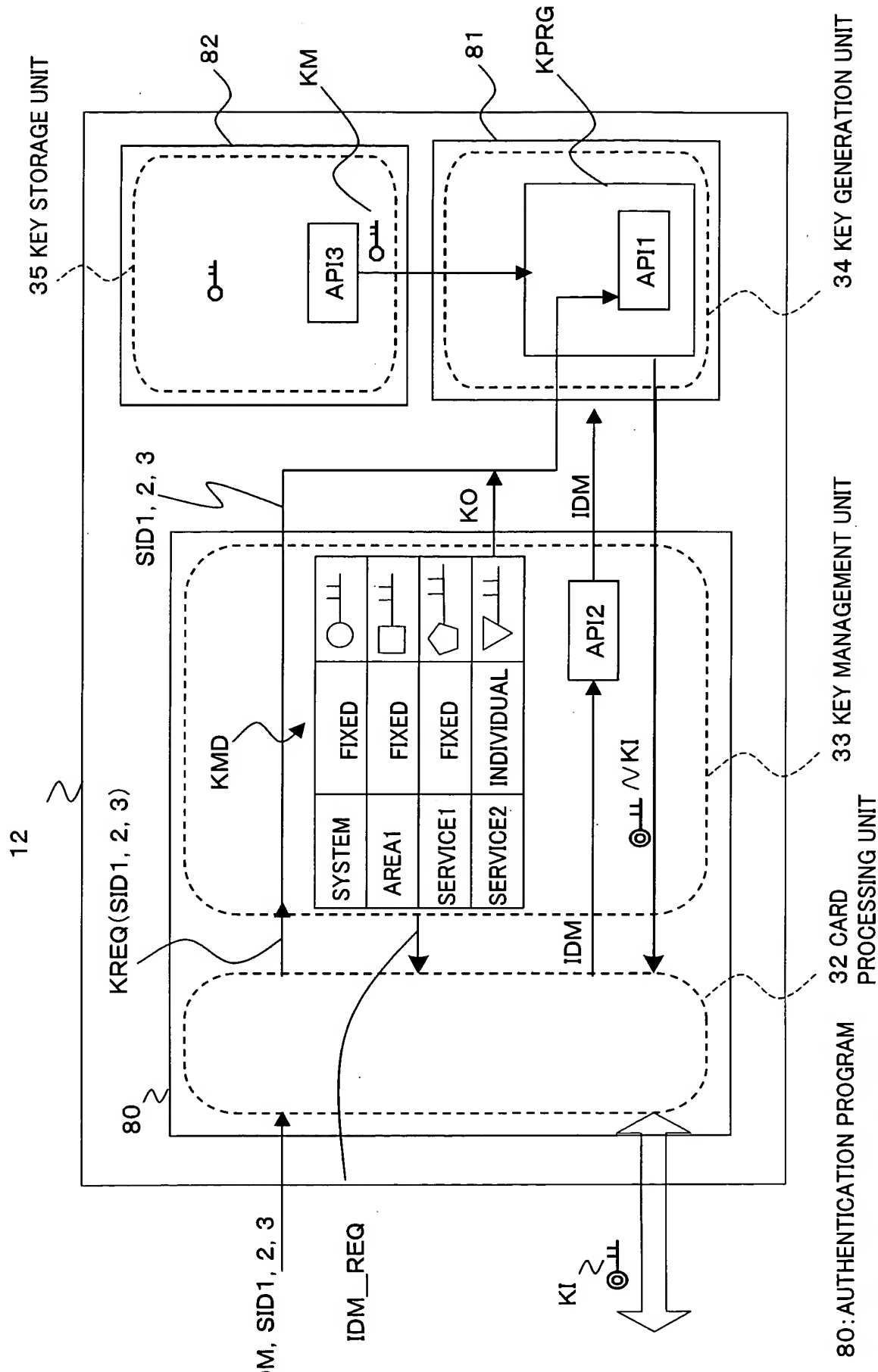

12
35 KEY STORAGE UNIT
82
KM
81
KPRG
API3
API1
34 KEY GENERATION UNIT
SID1, 2, 3
KO
IDM
KMD
SYSTEM
AREA1
SERVICE1
SERVICE2
FIXED
FIXED
FIXED
INDIVIDUAL
API2
KI
33 KEY MANAGEMENT UNIT
KREQ(SID1, 2, 3)
IDM
80
32 CARD PROCESSING UNIT
IDM, SID1, 2, 3
IDM_REQ
KI
80:AUTHENTICATION PROGRAM
81:KEY GENERATION PROGRAM
82:KEY HOLDING PROGRAM

FIG. 7

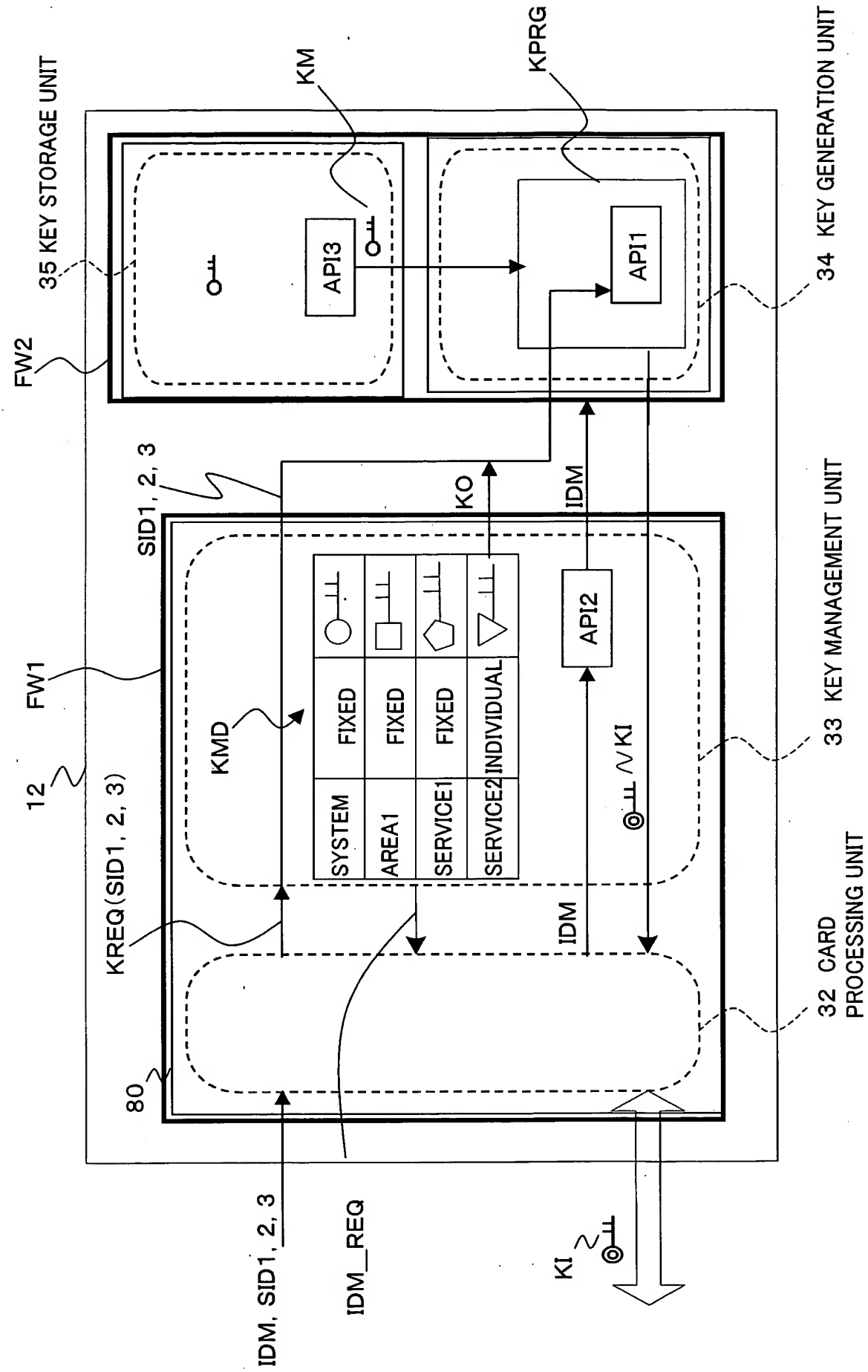

35 KEY STORAGE UNIT
KM
KPRG
API3
API1
34 KEY GENERATION UNIT
FW2
SID1, 2, 3
KO
IDM
FW1
12
KMD
SYSTEM
AREA1
FIXED
FIXED
SERVICE1
FIXED
SERVICE2
INDIVIDUAL
API2
KI
33 KEY MANAGEMENT UNIT
KREQ(SID1, 2, 3)
IDM
80
32 CARD PROCESSING UNIT
IDM, SID1, 2, 3
IDM_REQ
KI

FIG. 8

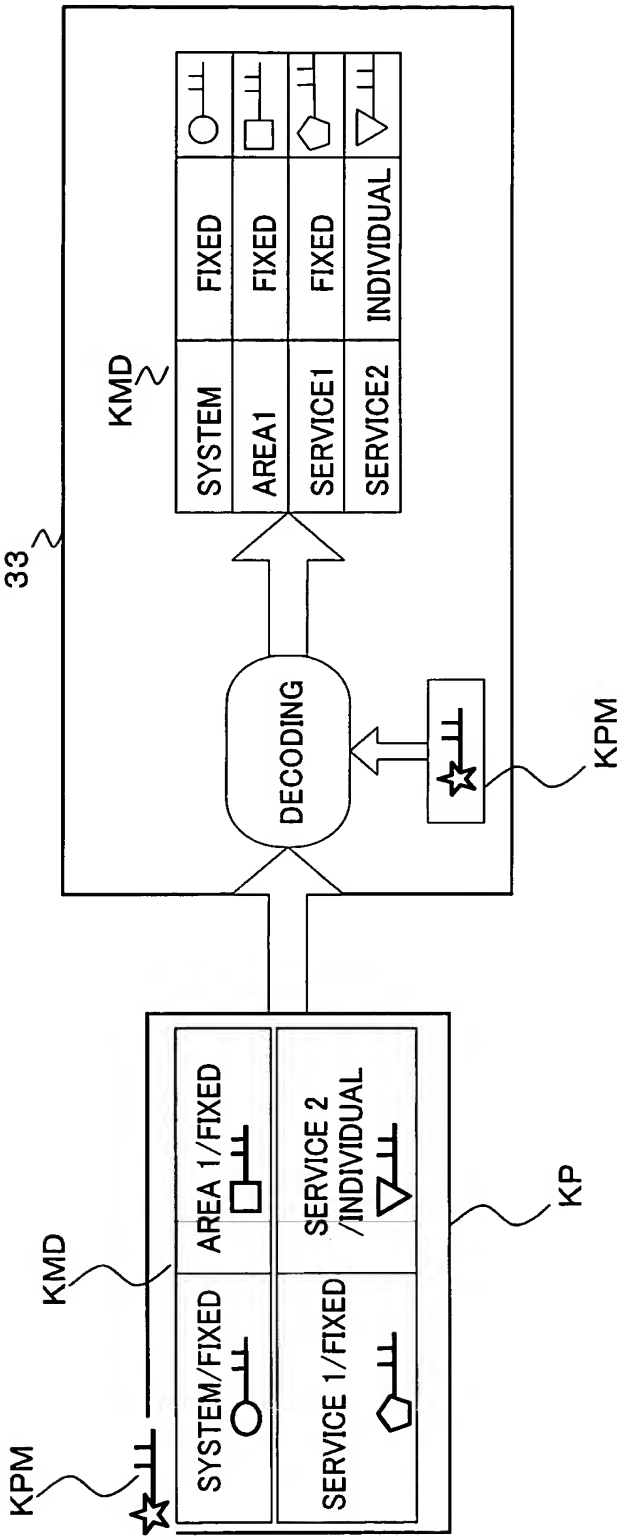

KMD
SYSTEM
AREA1
SERVICE1
SERVICE2
FIXED
FIXED
FIXED
INDIVIDUAL
33
DECODING
KPM
KMD
SYSTEM/FIXED
AREA 1/FIXED
SERVICE 1/FIXED
SERVICE 2
/INDIVIDUAL
KP
KPM
KMD:KEY MANAGEMENT DATA
KP:KEY PACKAGE

FIG. 9

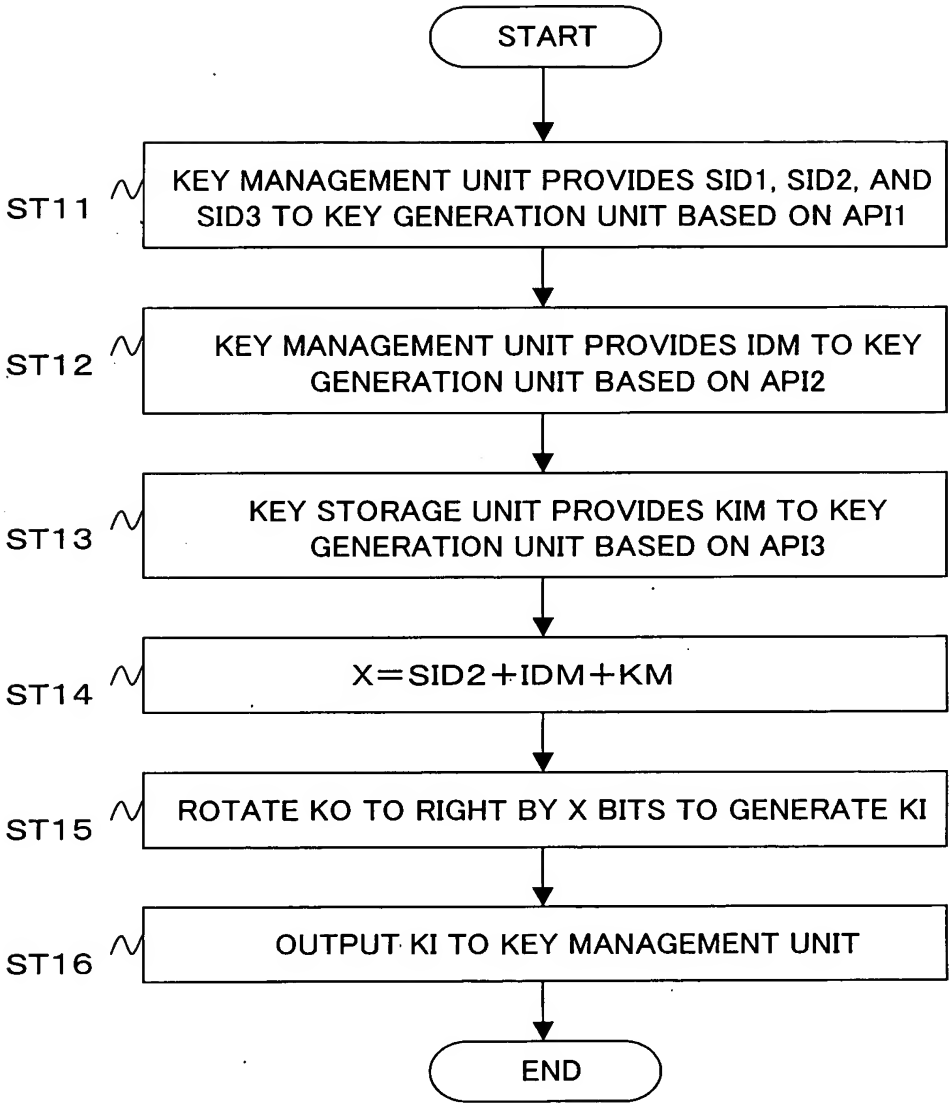

START
ST11
KEY MANAGEMENT UNIT PROVIDES SID1, SID2, AND SID3 TO KEY GENERATION UNIT BASED ON API1
ST12
KEY MANAGEMENT UNIT PROVIDES IDM TO KEY GENERATION UNIT BASED ON API2
ST13
KEY STORAGE UNIT PROVIDES KIM TO KEY GENERATION UNIT BASED ON API3
ST14
X=SID2+IDM+KM
ST15
ROTATE KO TO RIGHT BY X BITS TO GENERATE KI
ST16
OUTPUT KI TO KEY MANAGEMENT UNIT
END

FIG. 10

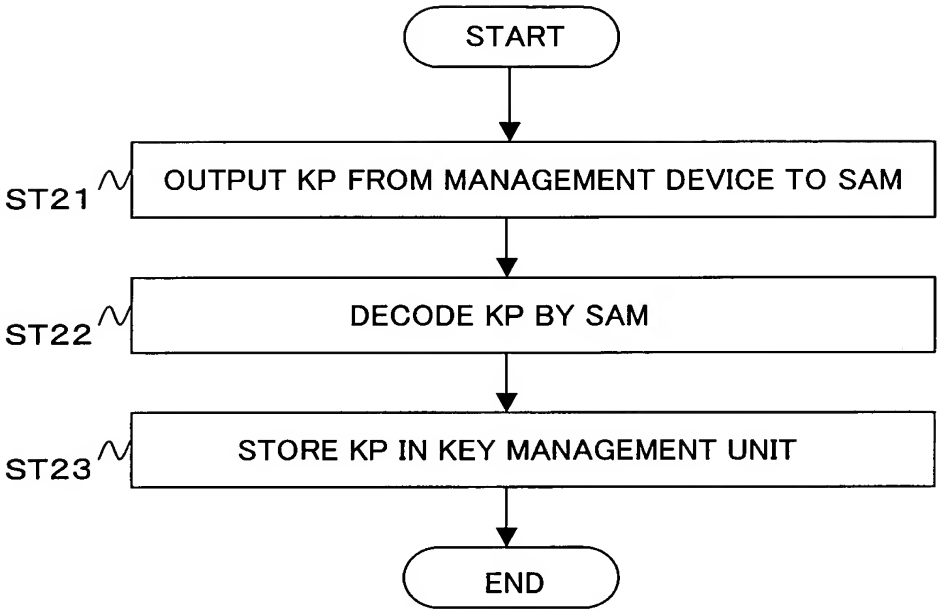

START
ST21
OUTPUT KP FROM MANAGEMENT DEVICE TO SAM
ST22
DECODE KP BY SAM
ST23
STORE KP IN KEY MANAGEMENT UNIT
END

FIG. 11

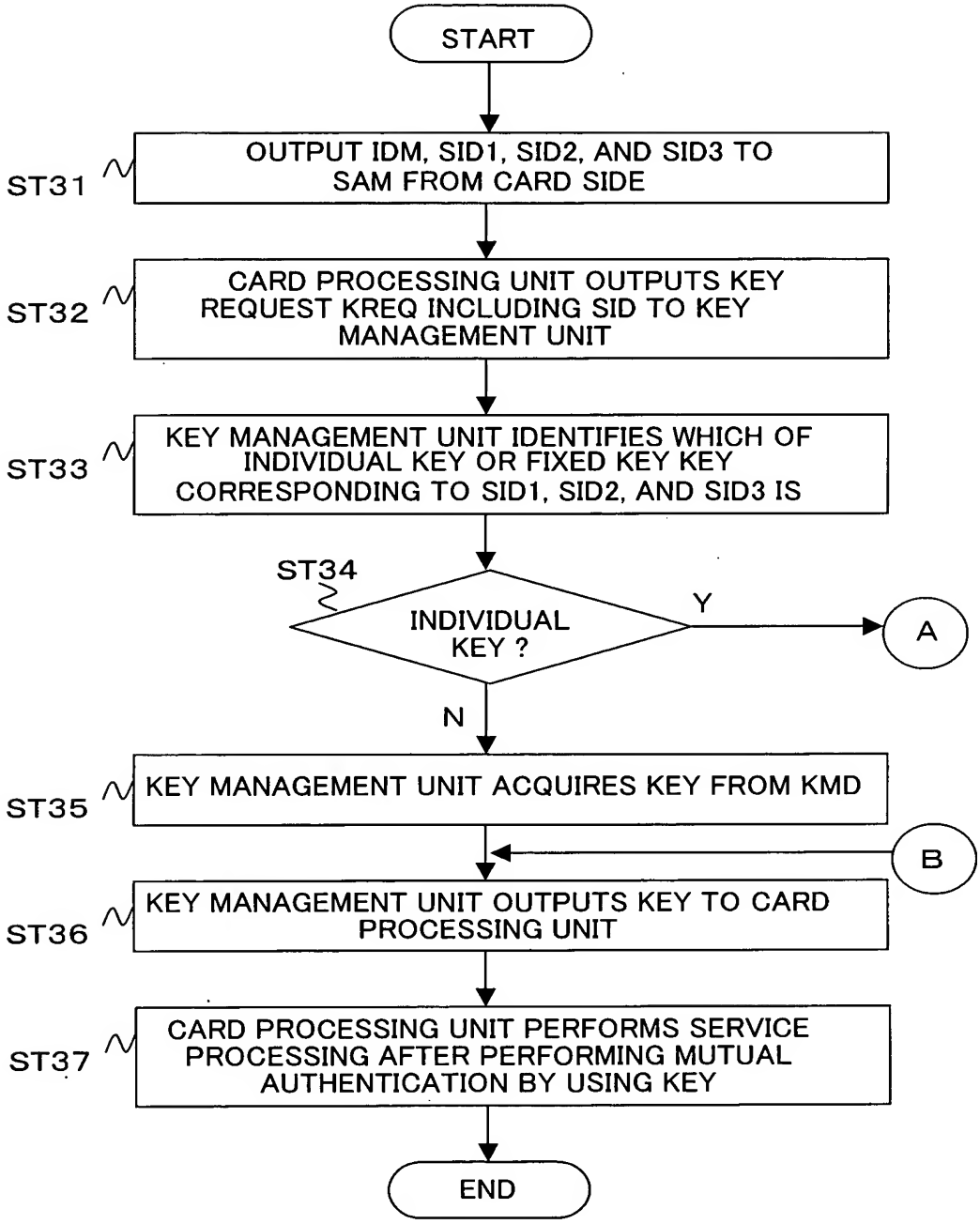
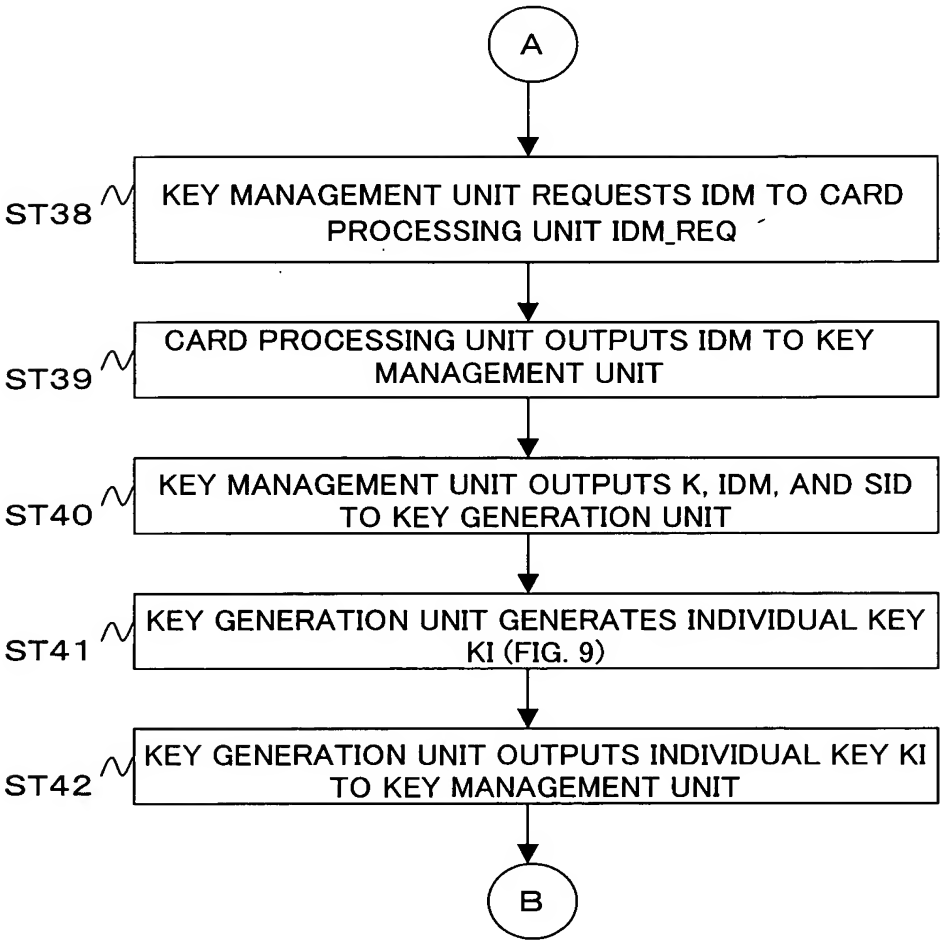

START
ST31
OUTPUT IDM, SID1, SID2, AND SID3 TO SAM FROM CARD SIDE
ST32
CARD PROCESSING UNIT OUTPUTS KEY REQUEST KREQ INCLUDING SID TO KEY MANAGEMENT UNIT
ST33
KEY MANAGEMENT UNIT IDENTIFIES WHICH OF INDIVIDUAL KEY OR FIXED KEY KEY CORRESPONDING TO SID1, SID2, AND SID3 IS
ST34
INDIVIDUAL KEY ?
Y
A
N
ST35
KEY MANAGEMENT UNIT ACQUIRES KEY FROM KMD
B
ST36
KEY MANAGEMENT UNIT OUTPUTS KEY TO CARD PROCESSING UNIT
ST37
CARD PROCESSING UNIT PERFORMS SERVICE PROCESSING AFTER PERFORMING MUTUAL AUTHENTICATION BY USING KEY
END

FIG. 12


A
ST38
KEY MANAGEMENT UNIT REQUESTS IDM TO CARD PROCESSING UNIT IDM_REQ
ST39
CARD PROCESSING UNIT OUTPUTS IDM TO KEY MANAGEMENT UNIT
ST40
KEY MANAGEMENT UNIT OUTPUTS K, IDM, AND SID TO KEY GENERATION UNIT
ST41
KEY GENERATION UNIT GENERATES INDIVIDUAL KEY KI (FIG. 9)
ST42
KEY GENERATION UNIT OUTPUTS INDIVIDUAL KEY KI TO KEY MANAGEMENT UNIT
B